UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/520,806	01/10/2005	Mehdi-Laurent Akkar	76.0726/PR	5077

41754 7590 04/07/2009
THE JANSSON FIRM
9501 N. CAPITAL OF TX HWY #202
AUSTIN, TX 78759

EXAMINER	
SCHWARTZ, DARREN B	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
04/07/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/520,806	**Applicant(s)** AKKAR ET AL.	
	Examiner DARREN SCHWARTZ	**Art Unit** 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 February 2009*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-6,8 and 9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-6,8 and 9* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Applicant amends claims 1, 2, 4-6 & 8, cancels claims 3 & 7, and adds claim 9.

Claims 1, 2, 4-6, 8 and 9 are presented for examination.

Response to Arguments

1. In light of the claim amendments, the claim objections are withdrawn, the 35 U.S.C 101 rejection is withdrawn and the previous grounds of 35 U.S.C 112 rejection is withdrawn.

Applicant's arguments with respect to claims 1, 2, 4-6, 8 and 9 have been considered but are moot in view of the new ground(s) of rejection.

The fact that the Examiner may not have specifically responded to any particular arguments made by Applicant and Applicant’s Representative, should not be construed as indicating Examiner’s agreement therewith.

Claim Objections

Claim 3 is objected to because of the following informalities:

Claim 3 recites “The method according to claim 1, further comprising move from E … and move from F’" and it is believed this should read "moving."

Claim 3 recites “… wherein h1 and h2 are mappings” and it is believed that claim should read “… wherein h_1 and h_2 are mappings.”

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1, 2, 4-6, 8 and 9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 6 and 8 recite the limitations “performing an elementary operation using a super-function operation acting from and/or to a larger set wherein a function f’ is super-function of a function f if $h_2(f'(h_1(x))) = f(x)$ wherein h_1 is a one-to-one mapping between a set E and a set E’ and h_2 is an onto mapping of a set F’ and a set F, wherein x is a member of E and f(x) is a member of the set F,” yet no limitation is provided if the conditional fails. This issue is raised because the “if” conditional, by its very nature, exhibits alternative steps in the event the “if" conditional fails; the alternative step(s) may, or may not, be limited to not performing any step(s). Ergo, the meets and bounds of the claim have not been clearly established. To remediate this issue, applicant must remove the conditional or include the alternative step(s) when the conditional fails.

Any claim not specifically addressed above is being rejected as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and

> the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 2, 4-6, 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lim (U.S. Pat Pub 2002/0003876 A1), hereinafter referred to as Lim, in view of Kocher (U.S. Pat 6539092 B1), hereinafter referred to as Kocher, as evidenced by Hein, James L. “Discrete Mathematics,” hereinafter referred to as Hein.

Re claim 1: Lim teaches a method to secure an electronic assembly implementing a calculation process:

performing an elementary operation using a super-function operation acting from and/or to a larger set wherein a function f’ is super-function [Fig 1, elt 130: see “48-Bit Input” and “32-Bit Output” and ¶10] of a function f [Fig1, elt CIPHER FUNCTION] if $h_2(f'(h_1(x))) = f(x)$ wherein h_1 [Fig 1, elt 110] is a one-to-one mapping [Fig 1, elt 110] between a set E [input 32-bit data] and a set E’ [output 48-bit data] (Lim: ¶8; Hein, page 92 teaches the definition of an injective or one-to-one function; one of ordinary skill will recognize an “expansion permutation” operation maps input bits to unique output bits thereby satisfying the conditions of being a one-to-one function) and h_2 [Fig 1, elt 140] is an onto mapping [Fig 1, elt 140] of a set F’ [input 32-bit data] and a set F [output 32-bit data] (Lim: ¶11; Hein, page 94 teaches “a function is called bijective if it is both injective and surjective” and also teaches on page 93 teaches a surjective function or onto function; one of ordinary skill will agree that a permutation operation is a bijective mapping as elements in the domain are uniquely mapped to elements in a co-domain, thereby satisfying the conditions of being a surjective function), wherein x [R(i-1), 32-bit data] is a member of E [32-bit data] and f(x) [Fig1, elt CIPHER FUNCTION] is a member of the set F [32-bit data].

However, Kocher teaches:

performing an additional calculation by a verification function on at least one intermediate result in order to obtain a calculation signature (col 6, lines 8-24 and col 7, lines 1-27);

performing the calculation by the verification function using the result obtained by the super function in order to obtain the calculation signature (col 6, lines 8-24 and col 7, lines 1-27).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Lim with the teachings of Kocher, for the purpose of preventing leaking of cryptographic operations (see at least Kocher: 54-58).

Re claim 2: The combination of Lim and Kocher teaches performing at least once more all or part of the calculation in order to recalculate said signature and compare them in order to detect a possible error (col 10, line 54 – col 11, line 23).

Re claim 4: The combination of Lim and Kocher teaches wherein the calculation of the elementary operation can be recomputed using the calculation of the super-function (col 10, line 54 – col 11, line 23).

Re claim 5: The combination of Lim and Kocher teaches:

move from E [input 32-bit data] to E' [output 48-bit data] by one-to-one function h_1 [Fig 1, elt 110] (Lim: ¶8; Hein, page 92 teaches the definition of an injective or one-to-one function; one of ordinary skill will recognize an "expansion permutation" operation maps input bits to unique output bits thereby satisfying the conditions of being a one-to-one function); and move from F' [input 32-bit data] to F [output 32-bit data] by onto function h2 [Fig 1, elt 140] (Lim: ¶11; Hein, page 94 teaches "a function is called bijective if it is both injective and surjective" and also teaches on page 93 teaches a surjective function or onto function; one of ordinary skill will agree that a permutation operation is a bijective mapping as elements in the domain are uniquely mapped to elements in a co-domain, thereby satisfying the conditions of being a surjective function); wherein h_1 and h_2 are mappings such that for any element x of E the following equality is true: $h_2(f'(h_1(x)))=f(x)$ [Fig1, elt CIPHER FUNCTION].

Re claims 6 and 8: Lim teaches an electronic assembly comprising a calculation process processing means, wherein the electronic assembly comprising storage means for storing instructions to cause the calculation processing (¶14; ¶30) and a smart card comprising storage means of a calculation process, processing means of said process (¶14; ¶30):

performing an elementary operation using a super-function operation acting from and/or to a larger set wherein a function f' is super-function [Fig 1, elt 130: see "48-Bit Input" and "32-Bit Output" and ¶10] of a function f [Fig1, elt CIPHER FUNCTION] if $h_2(f'(h_1(x)))=f(x)$ wherein h_1 [Fig 1, elt 110] is a one-to-one mapping [Fig 1, elt 110] between a set E [input 32-bit data] and a set E' [output 48-bit data] (Lim: ¶8; Hein, page 92 teaches the definition of an injective or one-to-one function; one of ordinary skill will recognize an "expansion permutation" operation maps input bits to unique output bits thereby satisfying the conditions of being a one-to-one function) and h_2 [Fig 1, elt 140] is an onto mapping [Fig 1, elt 140] of a set F' [input 32-bit data] and a set F [output 32-bit data] (Lim: ¶11; Hein, page 94 teaches "a function is called bijective if it is both injective and surjective" and also teaches on page 93 teaches a surjective function or onto function; one of ordinary skill will agree that a permutation operation is a bijective mapping as elements in the domain are uniquely mapped to elements in a co-domain, thereby satisfying the conditions of being a surjective function), wherein x [R(i-1), 32-bit data] is a member of E [32-bit data] and f(x) [Fig1, elt CIPHER FUNCTION] is a member of the set F [32-bit data].

However, Kocher teaches:

performing an additional calculation by a verification function on at least one intermediate result in order to obtain a calculation signature (col 6, lines 8-24 and col 7, lines 1-27);

performing the calculation by the verification function using the result obtained by the super function in order to obtain the calculation signature (col 6, lines 8-24 and col 7, lines 1-27).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Lim with the teachings of Kocher, for the purpose of preventing leaking of cryptographic operations (see at least Kocher: 54-58).

The combination of Lim and Kocher teaches an electronic assembly secured from differential attack and means to execute a verification function used to perform an additional calculation on intermediate results in order to obtain a calculation signature thereby securing the electronic assembly from differential attack (Kocher: Abstract and page 2, cited reference Biham).

Re claim 9: The combination of Lim and Kocher teaches the calculation of the elementary operation can be recomputed using the calculation of the super-function (Lim: Fig1, elt CIPHER FUNCTION contains elements 110, 130 & 140 as discussed *a priori*).

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the text of the passage taught by the prior art or disclosed by the examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Pat Pub 2005/0021990 A1

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARREN SCHWARTZ whose telephone number is (571)270-3850. The examiner can normally be reached on 8am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. S./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435